PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

CERTIFICATE OF MAILING

I hereby certify that the foregoing document is being deposited with the United States Postal Service as first class mail, postage prepaid, "Post Office to Addressee", in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA, 22313-1450 on May 17, 2010.

Anne E. Saturnelli

* * * * *

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Application Serial No.: 09/715,681

Filed: November 17, 2000

Applicants/Appellants: Yoav RAZ, et al.

Title: PHYSICAL SCANNING OF STORAGE BASED APPARATUS FOR ANTIVIRUS

Appeal from a decision of the Primary Examiner dated December 18, 2009

Atty. Docket: EMS-00202

REAL PARTY IN INTEREST

The above-identified application is assigned to EMC Corporation by virtue of an Assignment recorded by the U.S. Patent and Trademark Office on November 17, 2000, at Reel 011309 / Frame 0976.

RELATED APPEALS AND INTERFERENCES

Appellants are not aware of any other appeals or interferences related to the above identified application.

STATUS OF CLAIMS

This is an appeal from a decision of the Primary Examiner in the Final Office Action dated December 18, 2009 rejecting Claims 1, 3-7, 22, 24-28, 41, 43-52 and 63-71 in the above identified patent application. Claims 1, 3-7, 22, 24-28, 41, 43-52 and 63-71 are pending and stand rejected under 35 U.S.C. 103(a). Claims 2, 8-21, 23, 29-40, 42, and 53-62 have been canceled. No claim has been allowed or held allowable. Each of the pending Claims 1, 3-7, 22, 24-28, 41, 43-52 and 63-71 stands rejected and is appealed.

STATUS OF AMENDMENTS

A Final Office Action dated December 18, 2009 was received. A Notice of Appeal was filed on March 16, 2010. Accordingly, no amendments were filed subsequent to the Final Office Action dated December 18, 2009. The claims involved in this Appeal are set forth in the attached Claims Appendix.

SUMMARY OF CLAIMED SUBJECT MATTER

I. Background

A computer system may be attacked by so-called "viruses", which, in many instances, contain code that adversely affects operation of the computer system. Although viruses may exist as stand-alone data files, viruses may also be stored as part of an existing file and are sometimes hidden as seemingly innocuous parts of the file. Thus, a computer system may be infected with a virus by modifying a small portion of a file that is otherwise used for conventional operations unrelated to the virus. When the file is subsequently accessed, the virus may be activated and may cause damage to other parts of the computer system by, for example, replicating itself and/or destroying portions of other files on the computer system.

Antivirus software is provided by a number of commercial vendors to detect viruses on a computer system and, in some instances, remove the offending viruses. Most antivirus software works by scanning individual files to search for suspect patterns of known viruses. Thus, as new viruses are created and detected by the makers of antivirus software, the antivirus software is updated to take into account these new viruses and detect the corresponding patterns. Commercially-available antivirus software may be configured to operate on a single user computer. The antivirus software may run each time the computer is booted up and may scan each file for suspect patterns. However, it may be desirable to run antivirus software for one or more host processors that store and retrieve data using a multihost storage device containing a plurality of host interface units, disk drives, and disk interface units.

One way to perform antivirus checking on a multihost storage device is to run conventional single user antivirus software on each of the hosts so that files of the multihost storage device that belong to each host may be separately scanned by each host. However, such an arrangement may not provide for efficient coordination of the antivirus software for the entire multihost storage device. In addition, if one or more of the hosts do not properly run antivirus software, then viruses may exist on the multihost storage device even though other hosts have performed appropriate antivirus checking. In addition, such an arrangement may be inefficient with respect to updating the data base of known viruses when each of the hosts is separately updated with new virus information.

II. Appellants' Claimed Invention

Appellants' independent claims are discussed below in connection with the specification and Figures for purposes of example and explanation only in accordance with 37 C.F.R. 41.37(c)(v).

Claim 1 recites a computer implemented method of scanning a storage device for viruses, comprising: determining, by the storage device, each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device without using file-based information, the file-based information including information about file structure, file system, and file type (See, for example, page 15, lines 14-20; the multihost storage device 22 of Figure 4A; page 16, lines 4-12; use of the table 60 of Figure 5; page 17, lines 5-15; page 18, lines 7-17; page 19, lines 1-10); providing, to an antivirus unit by the storage device, information indicating which tracks of the storage

device have been accessed for a write operation since the previous virus scan (See, for example, use of the second line 58 of Figure 4A; page 16, lines 4-12 and lines 15-17; use of the table 60 of Figure 5; page 17, lines 5-15; page 18, lines 7-17; page 19, lines 1-10); and scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using the file-based information (See, for example, the antivirus unit 26 of Figure 4A; page 16, lines 4-12; use of the table 60 of Figure 5; page 17, lines 5-15; page 18, lines 7-17; page 19, lines 1-10).

Claim 66, which depends from Claim 1, recites wherein the antivirus unit is included in the storage device (See, for example, Figure 6, antivirus units 86, 87, 88 of device 22; page 18, line 18-page 19, line 11).

Claim 67, which depends from Claim 66, recites wherein the antivirus unit is included in a disk controller of the storage device (See, for example, Figure 6, antivirus units 86, 87, 88, respectively, of controllers 76, 77 and 78 in the device 22; page 18, line 18-page 19, line 11).

Claim 68, which depends from Claim 67, recites wherein the antivirus unit is included as software running on the disk controller (See, for example, Figure 6, antivirus units 86, 87, 88, respectively, of controllers 76, 77 and 78 in the device 22; page 18, line 18-page 19, line 11).

Claim 22 recites a computer program product for scanning a storage device for viruses, the computer program product including a computer-readable medium with executable code stored thereon for: determining, by the storage device, each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device without using file-based information, the file-based information including information about file structure, file system, and file type (See, for example, page 15, lines 14-20; the multihost storage device 22 of Figure 4A; page 16, lines 4-12; use of the table 60 of Figure 5; page 17, lines 5-15; page 18, lines 7-17; page 19, lines 1-10); providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation since the previous virus scan (See, for example, use of the second line 58 of Figure 4A; page 16, lines 4-12 and lines 15-17; use of the table 60 of Figure 5; page 17, lines 5-15; page 18, lines 7-17; page 19, lines 1-10); and scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using the file-based information (See, for example, the antivirus unit 26 of Figure 4A; page 16, lines 4-12; use of the table 60 of Figure 5; page 17, lines 5-15; page 18, lines 4-17; page 19, lines 1-10).

Claim 41 recites an antivirus unit, comprising: means for coupling to at least one storage device (See, for example, 56 and/or 58 of Figure 4A; page 16, lines 4-9 and lines 15-17); means for determining each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device

without using file-based information, the file-based information including information about file structure, file system, and file type (See, for example, page 15, lines 14-20; the antivirus unit 26 and device 22 of Figure 4A; page 16, lines 4-12; use of the table 60 of Figure 5; page 17, lines 5-15; page 18, lines 7-17; page 19, lines 1-10); means for receiving, from the at least one storage device, information determined by the at least one storage device indicating which tracks of the at least one storage device have been accessed for a write operation since the previous virus scan (See, for example, the antivirus unit 26 receiving information from the device 22 over 58 of Figure 4A; page 16, lines 4-12 and lines 15-17; use of the table 60 of Figure 5; page 17, lines 5-15; page 18, lines 7-17; page 19, lines 1-10); and means for scanning, using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using the file-based information (See, for example, the antivirus unit 26 of Figure 4A; page 16, lines 4-12; use of the table 60 of Figure 5; page 17, lines 5-15; page 18, lines 7-17; page 19, lines 1-10).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Claims 1, 3-4, 22, 24, 25, 41, 43, 44, 46-52, 63-66 and 71 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,928,555 to Drew in view of Stang (Stang, David, "Comparison: Products to Detect changes to Program", 1991).

II. Claims 5-7, 26-28, and 45 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,928,555 to Drew in view of Stang (Stang,

David, "Comparison: Products to Detect changes to Program", 1991), and further in view of U.S. Patent No. 6,094,731 to Waldin et al.

III. Claims 67-70 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,928,555 to Drew in view of Stang (Stang, David, "Comparison: Products to Detect changes to Program", 1991), and further in view of U.S. Patent No. 6,802,028 to Ruff et al..

ARGUMENT

I. The Examiner has failed to establish a prima-facie case of obviousness under 35 U.S.C. §103(a) of Claims 1, 3-4, 22, 24, 25, 41, 43, 44, 46-52, 63-66 and 71 as being unpatentable over U.S. Patent No. 6,928,555 to Drew in view of Stang (Stang, David, "Comparison: Products to Detect changes to Program", 1991).

A. Obviousness Standard

In determining whether or not there is a proper case of obviousness, it is necessary to establish whether one of ordinary skill in the art would, having the prior art references before him, be capable, or otherwise motivated, to make the proposed combination, modification or substitution so as to yield all elements of a claimed invention. *See KSR Int'l Corp. v. Teleflex Inc.*, 127 S. Ct. 1727, 82 USPQ2d 1385 (2007); *see also In re Lintner*, 458 F.2d 1013, 1016 (CCPA, 1972). In rejecting claims under 35 U.S.C. §103, it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness and the Examiner is expected to make the factual determinations set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 17, 148 USPQ 459, 467 (1966). *See also United States v. Adams,* 383

U.S. 39 (1966); *Anderson's-Black Rock, Inc. v. Pavement Salvage Co.*, 396 U.S. 57 (1969); and *Sakraida v. AG Pro, Inc.*, 425 U.S. 273 (1976). The analysis used to combine prior art teachings to invalidate a patent claim based on obviousness should be explicitly articulated. *See KSR*, 82 USPQ2d at 1396, citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness"). However, the analysis may take account of the inferences and creative steps that a person of ordinary skill in the art would employ. Id.

Furthermore, if a proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *See In re Gordon*, 733 F.2d 900, 902, 221 USPQ 1125, 1127 (Fed. Cir. 1984). In addition, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *See In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

B. The cited references of U.S. Patent No. 6,928,555 to Drew and Stang (Stang, David, "Comparison: Products to Detect changes to Program", 1991) do not disclose or fairly suggest every element of Appellants'claimed invention as to have rendered Appellants' claimed invention obvious to one of ordinary skill in the art at the time the invention was made.

The Examiner rejects Claims 1, 3-4, 22, 24, 25, 41, 43, 44, 46-52, 63-66 and 71 under 35 U.S.C. 103(a) as being obvious over U.S. Patent No. 6,928,555 to Drew (hereinafter referred to as "Drew") in view of Stang (Stang, David, "Comparison: Products to Detect changes to Program", 1991). Appellants traverse this rejection as set forth below and respectfully request that the rejection be reversed.

In following paragraphs, reference made to a Final Office Action refers to the Final Office Action dated December 18, 2009 unless otherwise noted.

Page 3 of the Final Office Action appears to erroneously indicate this rejection as applied to Claims 1, 3-7, 22, 24-28, 41, 44-52, 63-66, and 71. However, as best Appellant can determine based on additional detail supporting the claim rejections set forth on subsequent pages in the Final Office Action and existing claim dependencies, this rejection appears to apply to Claims 1, 3-4, 22, 24, 25, 41, 43, 44, 46-52, 63-66 and 71 as will be addressed below. The foregoing was also noted previously in the Response filed September 8, 2009 with respect to the Non-Final Office Action of June 16, 2009. No correction or indication to the contrary was made by the Examiner in the subsequent Final Office Action.

The Drew reference discloses a method and apparatus for minimizing file scanning by anti-virus programs. Col. 3, lines 40-55 and col. 4, lines 5-25 of Drew are cited by the Final Office Action as support for disclosing determining, by a storage device, each track of the storage device that has been accessed for a write operation since a previous scan using information about tracks of the storage device; providing to an antivirus unit by the storage

device information indicating which tracks of the storage device have been accessed for a write operation since the previous scan; and scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous scan for viruses. Col. 3, lines 40-55 of Drew refer to steps of the flowchart of Drew's Figure 2 with respect to processing performed with reference to Figure 1 in which an antivirus program is included in the network server computer 4. Col. 4, lines 5-25 of Drew disclose additional steps concerning determining whether a file was actually written that is modified by the user performing some writing step on the open file. The Final Office Action states that Drew is silent on the determining step being performed without using file-based information, the file-based information including information about a file structure, a file system and a file type, and performing scanning without using the filed-based information.

The Final Office Action cites to Stang as teaching determining physical portions of the storage device that have been modified since a previous virus scan using information about the physical portions without using the file-based information which includes information about file structure, file system and file type, and performing scanning without using the file-based information, citing to page 15, section Checkup of Stang,

Appellants' independent claims recite a computer-implemented method, computer-program product and antivirus unit that include at least the features of determining, by the storage device, each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device without using

file-based information, the file-based information including information about file structure, file system, and file type; and scanning, using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using the file-based information.

Appellants respectfully submit that the references, taken alone or in any combination, do not disclose or fairly suggest at least the above-noted features as recited in the independent claims. The Final Office Action states that Drew is silent concerning the above-noted features (see pages 3-4 of the Final Office Action) and cites to Stang as disclosing determining and scanning steps without using filed-based information, the file-based information including information about file structure, file system and file type. However, in contrast to that as contended by the Final Office Action for reasons set forth in more detail below, it is respectfully submitted that Stang does not disclose or fairly suggest at least the above-noted features of the independent claims.

As indicated above, the Final Office Action contends that Stang, page 15, section Checkup, discloses the above-noted features of Appellant's independent Claims. Page 15, section Checkup of Stang, states:

Checkup

> Checkup simply processes everything on your hard disk, and does not work from any input list. There is no upper limit on the number of files that can be scanned, other than your patience. Checkup is happy to point out that files have been changed, when they haven't been. This occurs because Checkup creates one X.XUP for every file beginning with X. Thus the signature for X.BAT is stored in X.XUPand the

```
signatures for X.COM, X.SYS, X.BAK, etc. are
compared with the contents of this file. With perhaps
10% of such "claims" wrong, you will lose patience with
it quickly. Checkup gets a 10 for efficiency, a 0 for
accuracy.
```

The foregoing citation of Stang merely indicates that the Checkup program or product performs checking of all files on the hard disk without using an input list of files. However, based on the disclosure in Stang, Checkup appears to still operate on files although it checks all such files on the hard disk. As noted in the above citation, Checkup points out "files" that have been changed and Checkup "creates one X.XUP for every file beginning with X". Thus, Checkup as disclosed by Stang appears to use filed-based information, such as at least file structure and/or file system information. In order for Checkup to determine and point out files that have changed, filed-based information, such as at least file structure and/or file system information, has to be used otherwise Checkup would not be able to perform such processing.

Furthermore, the foregoing portion of page 15 of Stang discloses that, with Checkup, file signatures are stored and compared to determine changes in file contents. The Checkup program as disclosed in Stang may scan an entire hard disk, but operates on files by determining and comparing file signatures. Thus, the Checkup program as disclosed in Stang operates on files and uses information about files in order to determine what is scanned. For example, in order to determine a signature for a file, the Checkup program of Stang must know file-based information about that file such as, for example, its location, size, etc.

Additionally, Stang discloses that Checkup is one program evaluated to catch a virus where the operation of Checkup on page 3 of Stang (section CRC-AWARE VIRUSES) is described as follows:

```
Programs could catch such a virus by using an incremental
cyclic redundancy check approach. In this approach, files are
dissected into randomly-sized blocks of data, using dynamic
block size allocations that allow files as small as one byte to be
accurately checked. CHECKUP uses this approach. It scans and
compares every byte of the target files on a block-by-block basis.
If the recorded file sizes, any of the block CRC comparisons, or
the CRC totals do not match, CHECKUP alerts users that the
target files have been altered.
```

As described above, Checkup dissects files into randomly sized blocks of data. Thus, Checkup appears to obtain information about what files exist on a drive and then dissects those files. The foregoing description of Checkup indicates that file-based information, such as information about file structure and/or file system is utilized in order to determine what files exist, file location and/or size in order to perform the disclosed dissecting, and the like. Furthermore, in addition to the foregoing portion of Stang explicitly stating that Checkup alerts a user that a target ***file*** has been altered, the foregoing portion also provides insight into the processing performed by Stang by indicating that a target file is determined as altered if the recorded file size, any of the block CRC comparisons, or the CRC totals do not match. Thus, the Checkup program performs processing to determine if a file has been altered using information including file size. Information such as file size is file based information such as file structure information and/or file system information. Therefore, Stang discloses determining which files have changed using file-based information such as including file size. The foregoing is in distinct contrast to the above-noted features recited in Claim 1 where the determining and scanning steps are performed without using the recited file-based information.

Furthermore, it is respectfully submitted that the recited determining step determines tracks accessed for a write operation since a previous scan and provides such information which is then used in the scanning step. Stang neither discloses nor suggests such a use. The Checkup program is described in Stang at page 15 as pointing out which files have changed after examining all files on the hard disk. Thus, Stang does not disclose or suggest determining tracks that have changed or have been accessed for a write operation and then using information about the foregoing in connection with scanning. Rather, Stang discloses that Checkup alerts users to what files have changed or have been altered. Stang does not disclose or suggest a determining step in which tracks written to since a previous scan are determined, and then performing scanning where the scanning uses information about such tracks that have been written to as determined from the determining step.

The Final Office Action appears to contend (see, for example, pages 2 and 4 of the Office Action) that Stang discloses scanning every file on the hard drive regardless of type, structure or system, and that Stang therefore discloses performing the recited determining step without using file-based information and performing scanning without using the file-based information. Appellants respectfully disagree. Stang appears to disclose processing all files on the hard disk. However, assuming for purposes of argument only, that this discloses or suggests "scanning every file on the hard drive regardless of type, structure or system", there is still no disclosure or suggestion in Stang of performing the recited determining without using file-based information and performing the recited scanning without using the file-based information. The mere fact that all files may be processed or that Stang's

processing may be performed "regardless of type, structure or system" does not disclose or suggest performing the recited determining and scanning without using the file-based information.

Thus, the references do not disclose or fairly suggest the above-noted features as recited in the independent claims. For at least the foregoing reasons, the references do not disclose or suggest the independent claims, and claims that depend therefrom.

Accordingly, Appellants respectfully submit that neither Drew nor Stang, taken alone or in any combination, disclose or fairly suggest at least the above-noted features of Claim 1, and claims that depend therefrom. Independent Claims 22 and 41 recite features similar to those above-noted features of Claim 1 pointed out above which are not disclosed or suggested by the references. Thus, Claims 22 and 41, and claims that depend therefrom, are also neither disclosed nor suggested by the references, taken separately or in combination, for reasons similar to those set forth above regarding Claim 1.

For at least those reasons set forth above, it is requested that the Board reverse the Examiner's rejection under 35 U.S.C. 103(a).

II. The Examiner has failed to establish a prima-facie case of obviousness under 35 U.S.C. §103(a) of Claims 5-7, 26-28 and 45 as being unpatentable over U.S. Patent No. 6,928,555 to Drew in view of Stang ("Comparison: Products to Detect

Changes to Programs") and further in view of U.S. Patent No. 6,094,731 to Waldin et al.

A. Standard Regarding Obviousness and Claim Interpretation

The standard regarding obviousness and claim interpretation is set forth above in connection with a previous rejection under 35 U.S.C. 103.

B. The cited references of Drew (U.S. Patent No. 6,928,555) and Stang ("Comparison: Products to Detect Changes to Programs") and further in view of Waldin et al. (U. S. Patent No. 6,094,731) do not disclose or fairly suggest every element of Appellants' claimed invention as to have rendered Appellants' claimed invention obvious to one of ordinary skill in the art at the time the invention was made.

The Examiner rejects Claims 5-7, 26-28 and 45 under 35 U.S.C. 103(a) as being obvious over Drew and Stang, and further in view of U. S. Patent No. 6,094,731 to Waldin et al. (hereinafter "Waldin"). Appellants traverse this rejection as set forth below and respectfully request that the rejection be reversed.

It is noted that the bottom of page 4 of the Final Office Action appears to erroneously indicate this rejection as applied to Claims 1, 3-7, 22, 24-28, 41, 44-52, 63-66, and 71. However, as best Appellant can determine based on additional detail supporting the claim rejections set forth in the Final Office Action and existing claim dependencies, this rejection appears to apply to Claims 5-7, 26-28 and 45 as will be addressed below. The foregoing was also noted previously in the Response filed September 8, 2009 with respect to the Non-Final

Office Action of June 16, 2009. No correction or indication to the contrary was made by the Examiner in the subsequent Final Office Action.

The features of independent Claim 1 are discussed above with respect to Drew and Stang. Claims 5-7 depend from independent Claim 1. Claims 26-28 depend from independent Claim 22. Claim 45 depends from independent Claim 41. Waldin is cited as support for disclosing features of the dependent Claims 5-7, 26-28 and 45 which Drew and/or Stang fail to disclose. Waldin is silent regarding any disclosure or suggestion of the above-noted features of independent Claims 1, 22 and 45.

Appellants respectfully submit that Waldin does not overcome the above-mentioned deficiencies of Drew and Stang with respect to independent Claims 1, 22 and 45. Appellants point out that nothing in Waldin corrects the deficiencies of Drew and Stang, as pointed out above with respect to at least the above-noted features as recited in Claims 1, 22 and 45 and as discussed above. Thus, combining Drew and Stang with Waldin does not overcome the deficiencies of Drew and Stang with respect to the foregoing features of Appellants' Claims 1, 22, 45, and claims that depend therefrom.

Claims 5-7, 26-28 and 45 which depend, respectively, from independent Claims 1, 22 and 41 are neither disclosed nor suggested by the references for at least the same reasons as Claims 1, 22 and 45.

Accordingly, Appellants respectfully submit that Drew, Stang and Waldin, taken alone or in any combination, disclose or fairly suggest Claims 1, 22 and 45, and claims that depend therefrom. For at least those reasons set forth above, it is requested that the Board reverse the Examiner's rejection under 35 U.S.C. 103(a).

III. The Examiner has failed to establish a prima-facie case of obviousness under 35 U.S.C. §103(a) of Claims 67-70 as being unpatentable over U.S. Patent No. 6,928,555 to Drew in view of Stang ("Comparison: Products to Detect Changes to Programs") and further in view of U.S. Patent No. 6,802,028 to Ruff et al.

A. Standard Regarding Obviousness and Claim Interpretation

The standard regarding obviousness and claim interpretation is set forth above in connection with a previous rejection under 35 U.S.C. 103.

B. The cited references of Drew (U.S. Patent No. 6,928,555) and Stang ("Comparison: Products to Detect Changes to Programs") and further in view of Ruff et al. (U. S. Patent No. 6,802,028) do not disclose or fairly suggest every element of Appellants' claimed invention as to have rendered Appellants' claimed invention obvious to one of ordinary skill in the art at the time the invention was made.

The Examiner rejects Claims 67-70 under 35 U.S.C. 103(a) as being obvious over Drew and Stang, and further in view of U. S. Patent No. 6,802,028 to Ruff et al. (hereinafter

"Ruff"). Appellants traverse this rejection as set forth below and respectfully request that the rejection be reversed.

The features of independent Claim 1 are discussed above with respect to Drew and Stang. Claims 67-70 depend from independent Claim 1. Ruff is cited as support for disclosing features of the dependent Claims 67-70 which Drew and Stang fail to disclose. Appellants note that Col. 7, Line 53-Col. 8, Line 34 of Ruff is apparently cited as support for teaching an antivirus unit included in a disk controller of a storage device, wherein the disk controller is a first disk controller of a plurality of disk controllers included in the storage device, the antivirus unit is a first antivirus unit of a plurality of antivirus units included in the storage device and each of said plurality of disk controllers includes a different one of said plurality of antivirus units.

Appellants respectfully submit that Ruff does not overcome the above-mentioned deficiencies of Drew and Stang with respect to independent Claim 1. Appellants point out that nothing in Ruff corrects the deficiencies of Drew and Stang, as pointed out above with respect to at least the above-noted features as recited in Claim 1 and as discussed above. Thus, combining Drew and Stang with Ruff does not overcome the deficiencies of Drew and Stang with respect to the foregoing features of Appellants' Claim 1, and claims that depend therefrom.

Claims 67-70 which depend from Claim 1 are neither disclosed nor suggested by the references for at least the same reasons as Claim 1. However, Appellants will point out some

particular features of the dependent claims which are also neither disclosed nor suggested by the references.

Claim 67 recites, in relevant part, ***wherein the antivirus unit is included in a disk controller of the storage device.*** Claim 68 also recites, in relevant part, ***wherein the antivirus unit is included as software running on the disk controller.*** As support for disclosing features of Claims 67 and 68, Ruff at Col. 7, Line 53-Col. 8, Line 34 is cited. The foregoing citation refers to Ruff's Figure 3 which includes a virus detector 312 and virus remover 316 in a computer system 100. The detector 312 and remover 316 are separate from the controller 306. Page 6 of the Office Action states that "Ruff teaches an antivirus unit included in a disk controller ...". However, Appellant cannot locate where in Figure 3, or in the foregoing citation of Ruff, is there disclosure or suggestion of the foregoing features of Claims 67 and 68. In contrast, Ruff's Figure 3 illustrates the virus detector and remover as part of the computer system but not included in the controller.

Accordingly, Appellants respectfully submit that Drew, Stang and Ruff, taken alone or in any combination, disclose or fairly suggest Claim 1, and claims that depend therefrom. For at least those reasons set forth above, it is requested that the Board reverse the Examiner's rejection under 35 U.S.C. 103(a).

CONCLUSION

For the reasons set forth herein, it is respectfully requested that the Board reverse all of the Examiner's rejections under 35 U.S.C. 103.

Respectfully submitted,
MUIRHEAD AND SATURNELLI, LLC

Date: May 17, 2010

Anne E. Saturnelli
Registration No. 41,290

Muirhead and Saturnelli, LLC
200 Friberg Parkway, Suite 1001
Westborough, MA 01581
T: (508) 898-8601
F: (508) 898-8602

CLAIMS APPENDIX

The claims on Appeal are as follows:

1. (Previously Presented) A computer implemented method of scanning a storage device for viruses, comprising:

determining, by the storage device, each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device without using file-based information, the file-based information including information about file structure, file system, and file type;

providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation since the previous virus scan; and

scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using the file-based information.

2. (Cancelled)

3. (Previously presented) A method, according to claim 1, wherein the portion corresponds to a sector of the storage device.

4. (Previously presented) A method, according to claim 1, wherein the portion corresponds to a subportion of the storage device.

5. (Previously presented) A method, according to claim 1, wherein said determining each track of the storage device that has been modified includes:

creating a table that is indexed according to each track and has entries indicating whether a corresponding track has been modified, the entries being cleared after a virus scan to indicate that no tracks have been modified; and

setting a specific one of the entries in response to a corresponding track of the storage device being subject to a write operation.

6. (Original) A method, according to claim 5, wherein creating the table includes copying an other table provided by the storage device.

7. (Original) A method, according to claim 5, wherein creating the table includes using an other table provided by the storage device.

Claims 8 - 21 (Cancelled).

22. (Previously Presented) A computer program product for scanning a storage device for viruses, the computer program product including a computer-readable medium with executable code stored thereon for:

determining, by the storage device, each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of

the storage device without using file-based information, the file-based information including information about file structure, file system, and file type;

providing, to an antivirus unit by the storage device, information indicating which tracks of the storage device have been accessed for a write operation since the previous virus scan; and

scanning, by the antivirus unit using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using the file-based information.

23. (Cancelled)

24. (Previously presented) A computer program product, according to claim 22, wherein the portion corresponds to a sector of the storage device.

25. (Previously presented) A computer program product according to claim 22, wherein the portion corresponds to a subportion of the storage device.

26. (Previously presented) A computer program product, according to claim 22, wherein said code for determining each track of the storage device that has been modified includes code for:

creating a table that is indexed according to each track and has entries indicating whether a corresponding track has been modified, the entries being cleared after a virus scan to indicate that no tracks have been modified; and

setting a specific one of the entries in response to a corresponding track of the storage device being subject to a write operation.

27. (Previously presented) A computer program product, according to claim 26, wherein said code for creating the table includes code for copying an other table provided by the storage device.

28. (Previously presented) A computer program product, according to claim 26, wherein said code for creating the table includes code for using an other table provided by the storage device.

Claims 29 - 40 (Cancelled).

41. (Previously Presented) An antivirus unit, comprising:

means for coupling to at least one storage device;

means for determining each track of the storage device that has been accessed for a write operation since a previous virus scan using information about tracks of the storage device without using file-based information, the file-based information including information about file structure, file system, and file type;

means for receiving, from the at least one storage device, information determined by the at least one storage device indicating which tracks of the at least one storage device have been accessed for a write operation since the previous virus scan; and

means for scanning, using the information provided by the storage device, at least a portion of each track identified as having been accessed for a write operation since the previous virus scan for viruses, wherein scanning is performed without using the file-based information.

42. (Canceled)

43. (Previously presented) An antivirus unit, according to claim 41, wherein the portion corresponds to a sector of the storage device.

44. (Previously presented) An antivirus unit, according to claim 41, wherein the portion corresponds to a subportion of the storage device.

45. (Previously presented) An antivirus unit, according to claim 41, further comprising:

a table that is indexed according to each track and has entries indicating whether a corresponding track has been modified, the entries being cleared after a virus scan to indicate that no tracks have been modified; and

means for setting a specific one of the entries in response to a corresponding track of the storage device being subject to a write operation.

46. (Original) An antrivirus scanning unit, according to claim 41, wherein said means for coupling includes means for coupling to only one storage device.

47. (Original) An antivirus unit, according to claim 41, wherein said means for coupling includes means for coupling to more than one storage device.

48. (Original) An antivirus unit, according to claim 41, further comprising:
means for coupling to at least one host.

49. (Original) An antivirus unit, according to claim 48, wherein said antivirus unit is interposed between said at least one storage device and said at least one host.

50. (Original) An antivirus unit, according to claim 48, wherein said antivirus unit is implemented as a process running on the at least one host.

51. (Original) An antivirus unit, according to claim 41, wherein said antivirus unit is implemented using stand alone hardware.

52. (Original) An antivirus unit, according to claim 41, wherein at least a portion of the antivirus unit is provided on at least some controllers for the at least one storage device.

Claims 53 - 62 (Cancelled).

63. (Previously presented) The method of Claim 1, wherein said storage device includes one or more sectors, and the method further comprising:

determining, for each sector of said storage device for a current virus scan, whether said each sector has been modified since a previous scan; and

for said current virus scan, scanning only those sectors determined to have been modified since said previous scan.

64. (Previously presented) The computer program product of Claim 22, wherein said storage device includes one or more sectors, and the computer-readable medium further comprising code stored thereon for:

determining, for each sector of said storage device for a current virus scan, whether said each sector has been modified since a previous scan; and

scanning only those sectors determined to have been modified since said previous scan.

65. (Previously presented) The antivirus unit of Claim 41, wherein said storage device includes one or more sectors, and the antivirus unit further comprising:

means for determining, for each sector of said storage device for a current virus scan, whether said each sector has been modified since a previous scan; and

means for scanning only those sectors determined to have been modified since said previous scan.

66. (Previously presented) The method of Claim 1, wherein the antivirus unit is included in the storage device.

67. (Previously presented) The method of Claim 66, wherein the antivirus unit is included in a disk controller of the storage device.

68. (Previously presented) The method of Claim 67, wherein the antivirus unit is included as software running on the disk controller.

69. (Previously presented) The method of Claim 67, wherein the antivirus unit is configured to use at least a portion of hardware that is separate from hardware of the disk controller.

70. (Previously presented) The method of Claim 67, wherein the disk controller is a first disk controller of a plurality of disk controllers included in the storage device, the antivirus unit is a first antivirus unit of a plurality of antivirus units included in the storage device, and each of said plurality of disk controllers includes a different one of said plurality of antivirus units.

71. (Previously presented) The antivirus unit of Claim 41, wherein said antivirus unit accesses data on the at least one storage device over a first connection and the information is provided on a second connection different from the first connection between said antivirus unit and the at least one storage device.

RELATED PROCEEDINGS APPENDIX

None.

EVIDENCE APPENDIX

None.